Select

Requires close bounds checking

Sean Barnum, Cigital, Inc. [vita[1]]

Copyright © 2007 Cigital, Inc.

2007-04-04

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3267 bytes

Attack Category	• Malicious Input • Denial of Service
Vulnerability Category	• Buffer Overflow
Software Context	• Networking
Location	• sys/select.h
Description	The ability to increase the value of an integer can lead to changing bits that reside outside the memory allocated for that integer. select(int n, fd_set *readfds, fd_set *writefds, fd_set *exceptfds, struct timeval *timeout) allows for I/O multiplexing under both SRV4 and 4.3+BSD. The first argument, n, (can also be written as maxfdp1 or "max fd plus 1") represents the highest descriptor of any of the three descriptor sets. Adding one to the first argument can potentially cause a one bit heap overflow.
APIs	**Function Name** / **Comments** select() /
Method of Attack	If an attacker increases the rlimit (a data structure the describes resource information) for the number of open files past 1024, then the bits past the end of the fds_bits structure can be changed to create a denial-of-service condition or execution of arbitrary code.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** If an attacker is given root access and changes the rlimit, then the attack is possible. / Root permissions are required to change rlimit. Thus, a system that is vulnerable to / The buffer overflow will not occur if rlimit is managed correctly.

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

		this theoretical attack can be already be assumed to be compromised before the attack is carried out.	
Signature Details			
Examples of Incorrect Code			
Examples of Corrected Code			
Source References	• ITS4 Source Code Vulnerability Scanning Tool[2] • http://security-protocols.com/unixmanpages/select.2.html • W. Stevens, *Advanced Programming in the UNIX Environment*. Boston, MA: Addison-Wesley Professional, 1993, ISBN: 0201563177 • http://securityfocus.com/bid/10455/discuss		
Recommended Resource			
Discriminant Set	**Operating Systems**	• Windows (All) • UNIX (All)	
	Languages	• C • C++	

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com[1].

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com